

WHAT IS CLAIMED IS:

1. A method for secure communication comprising:  
generating a virtual private proxy based on an  
agreement between a first entity and a second entity;  
5 associating a first virtual private proxy with the  
first entity and a second virtual private proxy with the  
second entity;

monitoring data at the first virtual private proxy  
associated with the first entity;

10 determining whether the data violates the agreement;  
and

disallowing communication of the data from the first  
virtual private proxy to the second virtual private proxy  
when the data violates the agreement.

15 2. The method for secure communication according  
to Claim 1, wherein determining whether the data violates  
the agreement comprises:

examining the data with respect to the agreement at  
20 the first virtual private proxy;

determining whether the data is allowed by the  
agreement; and

indicating a violation when the data does not  
conform to the agreement.

25 3. The method for secure communication according  
to Claim 2, wherein generating the violation comprises:

generating an alarm based on the violation;  
communicating the alarm to an appropriate entity;

30 and  
logging the violation.

4. The method for secure communication according  
to Claim 3, wherein the appropriate entity is a systems

administrator and wherein disallowing the data comprises discarding the data when the data violates the agreement.

5           5.    The method for secure communication according to Claim 3, wherein the alarm comprises information associated with the violation.

10           6.    The method for secure communication according to Claim 1, wherein the first virtual private proxy comprises a logical representation of a logical access point between the first entity and a secure switch.

15           7.    The method for secure communication according to Claim 1, wherein the first virtual private proxy comprises a logical representation of a physical access point between the first entity and a secure switch.

20           8.    The method for secure communication according to Claim 1, wherein the agreement comprises types of data allowed.

25           9.    The method for secure communication according to Claim 8, wherein the agreement further comprises a transport protocol indication and a transport security protocol indication and wherein the type of data allowed comprises XML data.

30           10.   The method for secure communication according to Claim 9, wherein the agreement further comprises a document exchange protocol indication and a process specification document indication.

          11.   The method for secure communication according to Claim 1, wherein monitoring the data comprises

monitoring data received at the first virtual private proxy from the first entity.

- 5           12. The method for secure communication according to Claim 1, wherein monitoring the data comprises monitoring data received at the first virtual private proxy to be communicated to the first entity.

10040573-100001

13. A system for secure communication comprising:

means for generating a virtual private proxy based on an agreement between a first entity and a second entity;

5 means for associating a first virtual private proxy with the first entity and a second virtual private proxy with the second entity;

means for monitoring data at the first virtual private proxy associated with the first entity;

10 means for determining whether the data violates the agreement; and

means for disallowing communication of the data from the first virtual private proxy to the second virtual private proxy when the data violates the agreement.

15

1004653.F004

14. A system for secure communication comprising:  
logic stored on a medium and operable to:

generate a virtual private proxy based on an  
agreement between a first entity and a second entity;

associate a first virtual private proxy with  
the first entity and a second virtual private proxy with  
the second entity;

monitor data at the first virtual private proxy  
associated with the first entity;

determine whether the data violates the  
agreement; and

disallow communication of the data from the  
first virtual private proxy to the second virtual private  
proxy when the data violates the agreement.

15. The system for secure communication according  
to Claim 14, wherein the logic is further operable to:

examine the data with respect to the agreement at  
the first virtual private proxy;

determine whether the data is allowed by the  
agreement; and

indicate a violation when the data does not conform  
to the agreement.

16. The system for secure communication according  
to Claim 15, wherein the logic is further operable to:

generate an alarm based on the violation;

communicate the alarm to an appropriate entity; and  
log the violation.

17. The system for secure communication according  
to Claim 16, wherein the appropriate entity is a systems  
administrator and wherein the logic is further operable  
to discard the data when the data is disallowed.

18. The system for secure communication according to Claim 16, wherein the alarm comprises information associated with the violation.

19. The system for secure communication according to Claim 14, wherein the first virtual private proxy comprises a logical representation of a logical access point between the first entity and a secure switch.

20. The system for secure communication according to Claim 14, wherein the first virtual private proxy comprises a logical representation of a physical access point between the first entity and a secure switch.

21. The system for secure communication according to Claim 14, wherein the agreement comprises types of data allowed.

22. The system for secure communication according to Claim 21, wherein the agreement further comprises a transport protocol indication and a transport security protocol indication and wherein the type of data allowed comprises XML data.

23. The system for secure communication according to Claim 22, wherein the agreement further comprises a document exchange protocol indication and a process specification document indication.

24. The method for secure communication according to Claim 14, wherein the logic is further operable to monitor data received at the first virtual private proxy from the first entity.

25. The method for secure communication according to Claim 14, wherein the logic is further operable to monitor data received at the first virtual private proxy to be communicated to the first entity.

5

10040573.710201

26. A method for secure communication comprising:  
generating a first virtual private proxy associated  
with a first entity;  
5 generating a second virtual private proxy associated  
with a second entity;  
monitoring communications between the first virtual  
private proxy and the second virtual private proxy based  
on an agreement for electronic data exchange between the  
10 first and second entities; and  
responding to violations of the agreement based on  
the agreement.

27. The method according to Claim 26 and further  
15 comprising:  
determining a first profile associated with the  
first entity;  
determining a second profile associated with the  
second entity; and  
20 automatically generating the agreement based on the  
first and second profiles.

28. The method according to Claim 26 and further  
comprising:  
25 linking the first virtual private proxy to the  
second virtual private proxy over a link; and  
communicating data between the first virtual private  
proxy and the second virtual private proxy over the link.

29. The method according to Claim 28, wherein the  
link comprises a logical data link at a secure switch.



30. The method according to Claim 26, wherein the first virtual private proxy comprises a logical representation of a logical access point.

5 31. The method according to Claim 26, wherein the first virtual private proxy comprises a logical representation of a logical access point between the first entity and a secure switch.

10 32. The method according to Claim 26, wherein the first and second entities respectively comprise a business.

15 33. The method according to Claim 26, wherein the first profile comprises at least one indication of business information associated with the first entity.

20 34. The method according to Claim 26, wherein the first profile comprises a transport protocol and a messaging protocol.

25 35. The method according to Claim 34, wherein the first profile further comprises a transport security protocol and a specification document.

30 36. The method according to Claim 35, wherein the first profile further comprises a name and contact information associated with the first entity.

37. The method according to Claim 26, wherein determining the violation comprises:

examining the data with respect to the agreement at the first virtual private proxy;

determining whether the data is allowed by the agreement;

determining the violation when the data is not allowed by the agreement; and

5 communicating the data to the second virtual private proxy when the data is allowed by the agreement.

38. The method according to Claim 26, wherein responding to the violation comprises:

10 generating an alarm based on the violation;  
logging the violation; and  
discarding the data associated with the violation.

15 39. The method according to Claim 38, wherein responding to the violation further comprises forbidding communication between the first virtual private proxy and the second virtual private proxy.

40. A system for secure communication comprising:  
means for generating a first virtual private proxy  
associated with a first entity;

5 means for generating a second virtual private proxy  
associated with a second entity;

means for monitoring communications between the  
first virtual private proxy and the second virtual  
private proxy based on an agreement for electronic data  
exchange between the first and second entities; and

10 means for responding to violations of the agreement  
based on the agreement.

10040573-10001

41. A system for secure communication comprising:  
logic stored on storage and operable to:  
generate a first virtual private proxy  
associated with a first entity;  
5 generate a second virtual private proxy  
associated with a second entity;  
monitor communications between the first  
virtual private proxy and the second virtual private  
proxy based on an agreement for electronic data exchange  
between the first and second entities; and  
10 respond to violations of the agreement based on  
the agreement.

42. The system according to Claim 41, wherein the  
logic is further operable to:  
15 determine a first profile associated with the first  
entity;  
determine a second profile associated with the  
second entity; and  
20 automatically generate the agreement based on the  
first and second profiles.

43. The system according to Claim 41, wherein the  
logic is further operable to:  
25 link the first virtual private proxy to the second  
virtual private proxy over a link; and  
communicate data between the first virtual private  
proxy and the second virtual private proxy over the link.

44. The system according to Claim 43, wherein the  
link comprises a logical data link at a secure switch.  
30

45. The system according to Claim 41, wherein the first virtual private proxy comprises a logical representation of a logical access point.

5 46. The system according to Claim 41, wherein the first virtual private proxy comprises a logical representation of a logical access point between the first entity and a secure switch.

10 47. The system according to Claim 41, wherein the first and second entities respectively comprise a business.

15 48. The system according to Claim 41, wherein the first profile comprises at least one indication of business information associated with the first entity.

20 49. The system according to Claim 41, wherein the first profile comprises a transport protocol and a messaging protocol.

25 50. The system according to Claim 49, wherein the first profile further comprises a transport security protocol and a specification document.

51. The system according to Claim 50, wherein the first profile further comprises a name and contact information associated with the first entity.

30 52. The system according to Claim 41, wherein the logic is further operable to:

examine the data with respect to the agreement at the first virtual private proxy;

determine whether the data is allowed by the agreement;

determine the violation when the data is not allowed by the agreement; and

communicate the data to the second virtual private proxy when the data is allowed by the agreement.

53. The system according to Claim 41, wherein the logic is further operable to:

generate an alarm based on the violation;

log the violation; and

discard the data associated with the violation.

54. The system according to Claim 53, wherein the logic is further operable to forbid communication between the first virtual private proxy and the second virtual private proxy.

55. A method for secure communication comprising:  
generating a virtual private proxy based on an  
agreement between a first entity and a second entity;

5 wherein the agreement further comprises a document  
exchange protocol indication and a process specification  
document indication;

associating a first virtual private proxy with the  
first entity and a second virtual private proxy with the  
second entity;

10 wherein the first virtual private proxy comprises a  
logical representation of a logical access point between  
the first entity and a secure switch;

monitoring data at the first virtual private proxy  
associated with the first entity;

15 examining the data with respect to the agreement at  
the first virtual private proxy;

determining whether the data is allowed by the  
agreement;

20 indicating a violation when the data does not  
conform to the agreement; and

disallowing communication of the data from the first  
virtual private proxy to the second virtual private proxy  
when the data violates the agreement.